

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

APR 28 2017

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*An Apple iPhone With Serial Number C8QPPQBZG5MP
Located at: Arlington County Police Department's Property
Section at 1425 N. Courthouse Rd. in Arlington, VA 22201

Case No. 1:17-sw-221

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. § 1343
 18 U.S.C. § 1349

Offense Description
 Wire Fraud.
 Conspiracy to Commit Wire Fraud.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT.

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by:

AUSA Kellen Dwyer

Applicant's signature

Special Agent David L. Hitchcock, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 04/28/2017

 Theresa Carroll Buchanan
 United States Magistrate Judge
*Judge's signature*City and state: Alexandria, Virginia

The Honorable Theresa C. Buchanan, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

The electronic devices to be searched are an Apple iPhone with serial number C8QPPQBZG5MP, hereinafter the "TARGET IPHONE." The TARGET IPHONE currently is located at the Arlington County Police Department's Property Section at 1425 North Courthouse Road in Arlington, Virginia 22201.

This warrant authorizes the forensic examination of the TARGET IPHONE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the TARGET IPHONE described in Attachment A that relate to violations of Title 18, U.S. Code, §§ 1343 (wire fraud) and 1349 (conspiracy to commit wire fraud), and involve KAMARA and KAMARA co-conspirators, including:
 - a. All documents, communications or other information related to the gathering, purchase, theft, sale or use of identities and personal identifying information, including records of Internet activity, such as Internet Protocol (“IP”) addresses, browser history, caches, cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
 - b. All documents, communications or other information related to the transferring or attempted transferring, of money by wire, between bank accounts and/or by or between credit card processing accounts, including the nature, source, destination, and use of those funds.
 - c. All documents, communications or other information related to the purchase, creation, transmission, or use of stolen, falsified, or fake credit cards, debit cards or other access devices.
 - d. All documents, communications or other information related to the obtaining, using, selling, or transmitting of stolen, fake or falsified personal identifying information or financial information, including but not limited to names, Social Security numbers, dates of birth, addresses, credit card numbers, and bank accounts.
 - e. All documents, communications or other information related to the structuring or other concealment of transfers and/or withdrawals.
 - f. All documents, communications or other information regarding the usernames, phone numbers, emails, Skype or instant messenger names used by the co-conspirators and/or

their associates to transmit information, including personally identifiable information ("PII"), credit card numbers, and false identification documents used in the scheme.

g. All communications with co-conspirators and accomplices and all photographs showing members of the conspiracy.

2. Evidence of user attribution showing who used or owned the TARGET IPHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as flash memory or other media that can store data) and any photographic form.

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA**

Alexandria Division

IN THE MATTER OF THE SEARCH OF
AN APPLE IPHONE WITH SERIAL
NUMBER C8QPPQBZG5MP LOCATED
AT:

ARLINGTON COUNTY POLICE
DEPARTMENT'S PROPERTY SECTION AT
1425 NORTH COURTHOUSE ROAD IN
ARLINGTON, VIRGINIA 22201

Case No. 1:17-sw-221

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE TARGET IPHONE**

I, David L. Hitchcock, a Special Agent with the Federal Bureau of Investigation ("FBI"),
being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of an Apple iPhone with serial number C8QPPQBZG5MP (the "TARGET IPHONE") which is currently in law enforcement possession, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent with the FBI and have been so employed for seven years. I currently am assigned to investigate computer-related crimes. As such, I have participated in numerous investigations involving computer and high-technology-related crimes, including computer intrusions, Internet fraud, credit card fraud, and bank fraud. Through my FBI employment, I have received training in general law enforcement and in such specialized areas

as computer and white-collar crimes. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer intrusions and other financial crimes stated under federal law, including 18 U.S.C §§ 1343 and 1349 (Conspiracy to Commit Wire Fraud).

3. The facts and information contained in this Affidavit are based upon my training and experience, participation in this and other investigations, personal knowledge, and observations during the course of this investigation, as well as the observations of other special agents, police officers, and individuals involved in this investigation. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by review of the records, documents, and other physical evidence obtained during the course of the investigation. This Affidavit contains only the information necessary to support probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. This affidavit is submitted for the purpose of showing probable cause to believe that the TARGET IPHONE described in Attachment A and located at the Arlington County Police Department's Property Section at 1425 North Courthouse Road in Arlington, Virginia 22201, contain the evidence, contraband, fruits, and instrumentalities listed in Attachment B of violations of 18 U.S.C. §§ 1343 and 1349 (Conspiracy to Commit Wire Fraud).

5. In addition, the applied-for warrant would authorize the forensic examination of the TARGET IPHONE for the purpose of identifying electronically stored data that also is particularly described in Attachment B.

PROBABLE CAUSE

I. Summary of Probable Cause

6. As described in further detail below, probable cause exists to believe that the owner of the TARGET IPHONE, Musa KAMARA, has conspired with Alvin SERRY, Moussa SY, Maxx TAPP, and other co-conspirators (collectively, the “Defendants”), in a scheme in the Eastern District of Virginia and elsewhere to obtain stolen credit card and debit card (hereinafter, “payment card”) numbers and use them to make fraudulent purchases.

7. Specifically, as part of the conspiracy, the Defendants obtained from co-conspirators (often via email) stolen “Track 2” data and encoded that data onto gift cards, which could then be used to make fraudulent purchases. Track 2 data is shorthand for the data found on the magnetic stripe of a payment card. It generally includes, among other data, the payment card (most often a 15- or 16-digit number starting with a 3, 4, 5, or 6), as well as the card’s four-digit expiration date. Track 2 data commonly is utilized in financial transactions and is the most commonly exchanged information by those involved in the distribution of payment card numbers.

8. After the Defendants load the gift cards with stolen Track 2 data, the Defendants either use the cards to make in-person purchases themselves or provide the cards to co-conspirators who make in-person purchases. Such in-person purchases have occurred at various brick-and-mortar retailers in the Eastern District of Virginia and elsewhere.

9. From the retailers’ perspective, the gift cards that the Defendants and their co-conspirators present at the time of payment appear to be legitimate gift cards. Yet, as a result of the Defendants encoding stolen Track 2 data onto the gift cards, the cards function like payment cards when swiped at the point of sale. That is, when a retailer swipes a gift card that the

Defendants have encoded with stolen payment card data, the software at the point-of-sale terminal transmits the victims' payment card information to servers controlled by the financial institution that issued the payment card information. The card issuer then sends back to the retailer an electronic transmission approving or denying the transaction. If the transaction is approved, the purchase is charged to the victim's account.

10. Throughout the course of the conspiracy, the Defendants and their co-conspirators made multiple fraudulent purchases which, as described in the above paragraph, caused wire signals containing stolen payment card information to be sent across state lines, from the point of sale to the servers controlled by the issuing financial institution.

11. As a result, TAPP recently pled guilty in this Court to conspiring with KAMARA, SERRY, and SY to commit wire fraud (*see* 1:17cr86), and KAMARA, SERRY, and SY have been indicted by a grand jury in this District on charges of conspiracy to commit wire and bank fraud and conspiracy to commit access device fraud (*see* 1:17cr82).

12. As spelled out in more detail below, over the course of a multiyear investigation, law enforcement and seized and searched the smart phones of several members of the conspiracy and have searched a back-up of a smart phone used by KAMARA. These searches confirm that members of the conspiracy, including KAMARA, have used smart phones to send email and text messages in furtherance of the conspiracy. In particular, members of the conspiracy have used smart phones to send each other stolen credit and debit card information and to communicate and coordinate their plans to make fraudulent purchases using stolen credit and debit card information.

13. Because the evidence shows that KAMARA was a member of a conspiracy that used smart phones to further the conspiracy, and because the TARGET IPHONE was seized

from KAMARA's person, I submit that there is probable cause to search the TARGET IPHONE for the evidence listed in Attachment B, which concerns the charged conspiracy.

II. Use of Smart Phones to Further the Charged Conspiracy

A. Search of Prince George's County Hotel on or about February 28, 2014

14. On or about February 28, 2014, law enforcement officers responded to a hotel in Prince George's County, Maryland, for a report of a suspect, later determined to be SY, paying for a hotel room with a stolen payment card number.

15. When law enforcement officers arrived on scene they interviewed the manager of the hotel. The manager stated that SY had attempted to rent a room but the payment card he provided was declined. The manager then approached SY and requested a new payment card. SY provided a payment card, which the manager scanned and returned to SY.

16. However, the payment card SY had provided to the hotel manager had a number embedded on its magnetic stripe that differed from the number on the card's face, and the number embedded on the magnetic stripe belonged to a victim who had not authorized SY to make use of its payment card information. Once the victim was contacted by its financial institution, the victim contacted the hotel.

17. Law enforcement then knocked on the hotel room in which SY was staying. SY answered the door and gave consent for law enforcement to enter the room and retrieve the payment card that he had attempted to use to rent the room. While in the room, law enforcement found the card in question along with SY's identification and approximately five to ten other payment cards in SY's wallet.

18. Law enforcement determined that the magnetic stripe of the card used to purchase the room was embedded with a payment card number that belonged to the victim who had called

the hotel. SY then was arrested and the vehicle parked in the space assigned to his hotel room was impounded. During the impounding process, law enforcement found dozens of gift cards in the vehicle. Thirty-eight of those cards had payment card numbers embedded onto their magnetic stripes that differed from the numbers on the face of the cards, a fact which, based on my training and experience, I know to be highly indicative of fraud.

B. Search of Anne Arundel Hotel on or about March 29, 2015

19. On or about March 29, 2015, law enforcement officers arrived at a hotel in Hanover, Maryland, for a report of the odor of marijuana coming from two hotel rooms. It subsequently was discovered that both rooms were rented under TAPP's name.

20. When the officers arrived, they were unable to detect any smell of marijuana coming from either room. As a result, they proceeded to leave the premises. Before they left, however, hotel management identified a vehicle in the hotel parking lot as being associated with the aforementioned rooms. Law enforcement then ran the vehicle's vehicle identification number and temporary West Virginia license plate and determined that the vehicle was designated to be stopped due to its suspected involvement with criminal acts in or around Fairfax, Virginia. Later that day, law enforcement saw a group of five individuals about to get into the subject vehicle. Law enforcement then stopped the group and identified them. Two of the people in the group were SERRY and TAPP.

21. During this interaction, hotel management asked law enforcement to assist hotel staff in removing from the premises the individuals associated with the subject vehicle along with any other individuals in the subject hotel rooms on the basis that the hotel management was terminating the hotel rental contract due to violations of the rental agreement.

22. Law enforcement complied with the hotel's request. One of the rooms appeared to be unoccupied based on the fact that nobody answered the door when law enforcement knocked and announced their presence. Upon not hearing any answer, law enforcement entered the room in order to ensure the room, in fact, was vacant. Inside the room, law enforcement saw in plain sight approximately 30 to 40 gift cards lying around the room, a large stack of gift cards lying on the desk, two laptop computers, a payment card re-encoding machine, a payment card laminating machine, and a Samsung cellular telephone. Both hotel rooms that TAPP had rented were secured and law enforcement obtained search warrants for both rooms.

23. Ultimately, it was discovered that some of the gift cards found in the vacant hotel room had been embedded with payment card numbers.

Search of the Samsung Cellphone Recovered from the Hotel

24. Evidence recovered from the Samsung cellphone indicates that it belongs to SERRY, including that the user of the Samsung cellphone sent at least two text messages to others indicating that his email address is ALVINNNNN95@GMAIL.COM. And, the Instagram account and Snapchat account found on the cellphone were linked to Alvinnnnn95@gmail.com. Accordingly, I will hereinafter refer to the Samsung cellphone seized from the Anne Arundel hotel room as "SERRY'S ANNE ARUNDEL PHONE".

25. Items found within SERRY'S ANNE ARUNDEL PHONE relate to SY's involvement in the conspiracy, including numerous text messages between SERRY'S ANNE ARUNDEL PHONE and a contact listed as "Millz," For instance, on or about March 1 and 3, 2015, "Millz" sent text messages to the SERRY'S ANNE ARUNDEL PHONE that consisted of what appears to be Track 2 data. I believe that "Millz" is short for SY's alias, "Mugga Millz," because, among other things, I have viewed a Facebook

account in the name “Mugga Millz” with profile pictures matching SY, and I have tied the email address, MILLZ.MUGGA@YAHOO.COM to SY (see paragraph 35 and its subparts below).

Search of the Toshiba Laptop Recovered from the Hotel Room

26. Pursuant to the search warrants discussed above, law enforcement officers also seized a Toshiba laptop. A digital examination of the laptop was performed and the following evidence relating to the conspiracy was uncovered:

- a. A large quantity of Track 2 data was discovered throughout the laptop.
- b. Also found on the laptop were backup files for an iPhone 5 and an iPhone 5c.

Based on my training and experience, I know that data on iPhones can be backed up to a computer in order to preserve the data in the event the physical phone is damaged or misplaced.

c. It appears that the iPhone 5 backup file is associated with KAMARA for a number of reasons. First, the backup was entitled “Deen,” a known alias of KAMARA. Second, a Twitter account found within the backup includes photographs that appear to be of KAMARA and Twitter posts that appear to be KAMARA referencing himself. Third, text messages found within the backup file appear to refer to KAMARA as “Gadafi,” “Gadafi Deen,” or “Deen.” These nicknames are similar to a Facebook page for “King-Dafi Deen” that appears to include KAMARA’s picture as the account’s profile picture, and an Instagram account for “king_dafi” that includes a posting regarding a medical health record associated with KAMARA. Fourth, text messages from a phone number associated with an individual identified within the backup file as “mom,” repeatedly refer to the recipient of the messages as “Zainu,” which is KAMARA’s middle name. Finally, numerous photos within the backup are of KAMARA, often

in the style known as “selfie,” *i.e.*, a person’s taking of a photograph of themselves. Therefore, I will hereinafter refer to this phone backup as “KAMARA’S PHONE.”

27. KAMARA’S PHONE appears to contain evidence regarding the distribution and obtainment of payment card numbers belonging to third parties, including text messages between the user of KAMARA’S PHONE and a contact identified as “Millz,” who, as discussed below, is believed to be SY, that appear to relate to the use of gift cards. For instance, on or about September 15, 2014, Millz sent the following text message to KAMARA’S PHONE: “let me cash u out how many gcs u got.” The user of KAMARA’S PHONE responded that he only had 500 and he had space on his AMEX. Similarly, on or about September 20, 2014, Millz sent a text message to KAMARA’S PHONE asking whether he had “any gcs for sell,?”, to which the user of KAMARA’S PHONE responded that he was in Ohio.

C. Arlington Hotel Incident on or about May 21, 2015

28. On or about May 21, 2015, officers of the Arlington County Police Department were dispatched to a room at a hotel located in Arlington, Virginia, which is within the Eastern District of Virginia, in response to a report of an odor of marijuana emanating from the room. After knocking on the door to the hotel room, which had been rented by TAPP through the use of three gift cards, the officers encountered three individuals who now are known to be SERRY, TAPP, and V.C.¹

29. SERRY, TAPP, and V.C. consented to a search of the hotel room. During the ensuing search, the officers discovered approximately 90 gift cards outside of their packaging, a Toshiba laptop attached to a MSR606H magnetic stripe card reader/writer, and a Samsung

¹ V.C.’s true name is known to law enforcement. It is being withheld here for purposes of confidentiality.

cellphone with model number Samsung-SM-G920A. Based upon my training and experience, I know that a MSR606H magnetic stripe card reader/writer, when connected to a laptop, is capable of embedding a payment card number onto the magnetic stripe of a gift card.

30. During a consensual interview, SERRY did not claim ownership of either the Toshiba laptop or the Samsung cellphone. Yet, while outside the hotel room and in the presence of law enforcement, SERRY requested to reenter the hotel room in order to retrieve a charger.

Search of Toshiba Laptop Found in the Arlington Hotel Room

31. Pursuant to a search warrant obtained by the Arlington County police, law enforcement searched the Toshiba laptop found in the hotel room. That search revealed, *inter alia*, emails between MAGICBLUE95@GMAIL.COM and MILLZ.MUGGA@YAHOO.COM that contained what appears to be payment card numbers and the cities and states associated with each number. A total of nine suspected payment card numbers and associated data were discovered among the aforementioned emails. Moreover, three of these suspected payment cards numbers were found embedded on the magnetic stripes of three gift cards located within the hotel room. Law enforcement subsequently confirmed that all three numbers, in fact, were payment card numbers that had been stolen.

Search of Samsung Cellphone Found in the Arlington Hotel Room

32. Based on the search of the Samsung cellphone found within the Arlington hotel room, which was done pursuant to search warrant obtained by Arlington County police, it appears that the cellphone belongs to SERRY. This is so for the following reasons:

a. First, three cellphones were found within the hotel room in which officers encountered SERRY, TAPP, and V.C. on or about May 21, 2015. TAPP and V.C. claimed to

own two of those cellphones, but not the Samsung cellphone. Although SERRY claimed that another individual was staying in the room, there was no indication that anyone else, in fact, had occupied the room.

b. Second, law enforcement found text messages on the Samsung cellphone that was dated on or about May 10, 2015, and was between the Samsung cellphone and a contact listed as “Maxieeeee.” At least one text message from “Maxieeeee” referred to the Samsung cellphone user as “Alvin,” *i.e.*, SERRY’s first name. The phone number listed in the Samsung cellphone for Maxieeeee is the same as the telephone number that TAPP told law enforcement was hers during the interview that occurred on or about May 21, 2015.

c. Third, during the encounter at the Arlington hotel room on or about May 21, 2015, TAPP and SERRY indicated that they were in a relationship. Several of the text messages found on the Samsung cellphone are between “Maxieeeee” (again, who is believed to be TAPP) and the user of the cellphone, and the messages appear to be intimate in nature.

d. Fourth, law enforcement found a text message on the Samsung cellphone dated on or about May 15, 2015, in which the user of the Samsung cellphone sent a communication to a contact listed as “Ti” and referred to himself as “blue.” It is believed that “Blue” is one of SERRY’s aliases, based in part, on SERRY’s ownership of the account MAGICBLUE95@GMAIL.COM, as demonstrated in paragraph 32 and its subparts below.

e. Fifth, law enforcement subsequently searched the MAGICBLUE95@GMAIL.COM email account pursuant to a search warrant and found an email dated on or about May 9, 2015, that indicated the telephone number for the Snapchat account affiliated with MAGICBLUE95@GMAIL.COM had been changed to the telephone number assigned to the Samsung cellphone. As discussed below, it is believed that

MAGICBLUE95@GMAIL.COM is owned and controlled by SERRY. Therefore, hereinafter I will refer to this Samsung phone as “SERRY’S ARLINGTON PHONE.”

33. A review of the text messages on SERRY’S ARLINGTON PHONE uncovered communications indicative of SERRY and SY’s involvement in the conspiracy, including:

a. On or about May 17, 2015, the following communications were sent to SERRY’S ARLINGTON PHONE from TELEPHONE NUMBER 1:² “I pay expensive for my shyt n if u can’t knock 23 out in less than 3 hours I can’t d none with ya”; and “other made 8100 off 25.” It is believed that TELEPHONE NUMBER 1, which was associated in SERRY’S ARLINGTON PHONE with the name “Millz,” was SY’s telephone number on or about May 21, 2015. The basis for this belief is that, on or about July 6, 2015, SY was arrested by law enforcement in Maryland for trespassing and TELEPHONE NUMBER 1 was attributed to SY in the police report that was generated subsequently.

b. Also found on the Samsung cellphone were text messages from on or about May 21, 2015, in which TELEPHONE NUMBER 1, *i.e.*, “Millz,” and the Samsung cellphone user appear to discuss the Samsung cellphone user’s location and the transmittal of payment card numbers via email. The relevant portion of the text messages are as follows:

Millz:	Lol where YALL at
SERRY’S ARLINGTON PHONE:	At embassy suites
Millz:	Which one ?
SERRY’S ARLINGTON PHONE:	Innnnncrystal city wya bra

² The actual telephone number is known to law enforcement, but is being withheld here for purposes of confidentiality.

Millz: Germantown

Millz: Yea u read ?

SERRY'S ARLINGTON PHONE: Ready

SERRY'S ARLINGTON PHONE: Magicblue95@gmail.com

c. Furthermore, on or about May 21, 2015, the following text message was sent from TELEPHONE NUMBER 1 to the Samsung cellphone: "5 joints more than 2 hrs already no updates." Law enforcement found an email dated on or about May 21, 2015, that was sent from MUGGAMILLZ@YAHOO.COM to MAGICBLUE95@GMAIL.COM and contained five payment card numbers with points of origin listed as New York, New York. Of those numbers, at least three of them were confirmed to be stolen. Furthermore, all five of the numbers sent in the May 21 email were found embedded onto the magnetic stripes of gift cards located with the hotel room that was searched on or about May 21, 2015.

Search of TAPP's Cellphone

34. Pursuant to a search warrant obtained by Arlington County police, the iPhone found in the Arlington County hotel room and claimed by TAPP was searched and the following evidence relating to the conspiracy was uncovered:

a. A screenshot was found on TAPP's phone that stated from "millz to me." The screenshot, which appears to be from a Gmail account, lists a series of what appear to be payment card numbers. Markedly, this list is identical to an email sent from MILLZ.MUGGA@YAHOO.COM to MAGICBLUE95@GMAIL.COM on or about May 16, 2015.

b. Text messages between TAPP and TELEPHONE NUMBER 1 were found that appear to provide an update regarding TAPP's and others' use of the gift cards encoded with

third parties' Track 2 data. One such message from TAPP states: "3 did 900 one didn't work we on the way to the next store[.]"

Search of Email Accounts Connected to the Arlington Hotel Room Search

35. Pursuant to information learned during the aforementioned investigation, Arlington County police officers obtained and executed a search warrant on Google regarding the MAGICBLUE95@GMAIL.COM email account and a search warrant on Yahoo regarding the MILLZ.MUGGA@YAHOO.COM email account. It appears that these email accounts are SERRY's and SY's, respectively. This is so for the following reasons:

a. As stated above, a text message was found on SERRY'S ARLINGTON PHONE in which the user of the cellphone indicates that his email address is MAGICBLUE95@GMAIL.COM.

b. During an interview with SY's sister on or about June 10, 2016, she allowed law enforcement to review the contents of her telephone. SY was listed as one of her contacts and the email address associated with SY's contact was MILLZ.MUGGA@YAHOO.COM.

c. Records obtained from American Express identify MILLZ.MUGGA@YAHOO.COM as the email associated with an American Express account that appears to be SY's based on the personal information connected to the account.

d. Furthermore, an email was sent to MILLZ.MUGGA@YAHOO.COM from *hotwire.com* regarding a stay at hotel in Greenbelt, Maryland, from on or about July 5, 2015 to on or about July 6, 2015. SY was staying at this hotel on the dates mentioned at the time he was arrested for trespassing by Greenbelt law enforcement.

e. A confirmation email was sent from Saks Fifth Avenue to MILLZ.MUGGA@YAHOO.COM on or about January 1, 2015, regarding an order. The billing

and shipping address of the order was for “Moussa Sy” at 850 Quincy Street, NW, Washington, D.C.

36. An examination of MILLZ.MUGGA@YAHOO.COM also indicates that this account was used to carry out the wire fraud conspiracy with the assistance of others. This is so for the following reasons:

a. An examination of MILLZ.MUGGA@YAHOO.COM revealed that approximately 3,104 suspected payment card numbers (some of which appear to be duplicates) were sent to or from this email account.

b. Likewise, on or about or about March 13, 2015, an email was sent from MILLZ.MUGGA@YAHOO.COM to ALVINNNNN95@GMAIL.COM that contained what appears to be Track 2 data from a series of payment cards. It appears that the ALVINNNNN95@GMAIL.COM belongs to SERRY. This is because pursuant to a search warrant, law enforcement discovered numerous emails which contained SERRY’s résumés, his community college account, photographs of his Maryland Provisional Driver’s License, and various school papers that had SERRY’s name on them. Furthermore, records obtained from American Express revealed that ALVINNNNN95@GMAIL.COM is associated with an American Express account that is in SERRY’s name and is connected to his personal information.

c. In addition, on or about May 5, 2015, an email was sent from MILLZ.MUGGA@YAHOO.COM to KILMERST92@GMAIL.COM that contained a series of numbers that appear to be Track 2 payment card data. It appears that KILMERST92@GMAIL.COM belongs to KAMARA. This is because, pursuant to a search warrant, law enforcement obtained and searched the contents of KILMERST92@GMAIL.COM

and found an email from American Express that referred to KAMARA by name and multiple emails regarding hotel reservations that referred to KAMARA by name. Records obtained from American Express revealed that this email account is associated with an American Express account in KAMARA's name. Several emails found within this account were related to the purchasing of stolen credit card numbers. For example, an email was sent to the account on or about October 26, 2015, from the email address of REAL@HOB007.CA. It stated "Dear customer, our latest base Red October is available for the mixes with a mix prices already both in SecureIM & YBFStore!" Law enforcement knows that the term "base," is often slang for a group of credit card numbers that are for sale after being obtained through some type of illegal means.³ Two emails were found within the account which were from KILMERST92@GMAIL.COM to an unknown recipient, both of which contained the same four credit card numbers.

D. Search of SY's Residence in Beltsville, Maryland, on or about June 10, 2016

37. On or about June 10, 2016, law enforcement officers executed a search warrant on a residence in Beltsville, Maryland. Prior to obtaining and executing the search warrant, law enforcement officers conducted surveillance of the residence and identified SERRY as an individual who was entering and leaving the residence frequently.

38. Law enforcement discovered during the search of the Beltsville residence numerous laptops, an MSR6 magnetic stripe reader/writer, two payment card embossing machines, various cellphones, an identification maker, and approximately 340 payment cards and gift cards. Based upon my training and experience, I know that a MSR6 magnetic stripe card

³ Law enforcement also has found emails from REAL@HOB007.CA to MILLZ.MUGGA@YAHOO.COM that contain what appear to be fraudulently obtained payment card numbers.

reader/writer, when connected to a laptop, is capable of embedding a payment card number onto the magnetic stripe of a gift card.

39. By comparing the account numbers on the faces of the approximately 340 cards found within the residence to the account numbers on the cards' magnetic stripes, it was discovered that approximately 240 cards had account numbers embedded on their magnetic stripes that were different from the account numbers on their faces.

Search of the Samsung Cellphone Found in the Beltsville Residence

40. One of the cellphones found during the Beltsville search was a Samsung cellphone. Pursuant to a search warrant, law enforcement reviewed the contents of the Samsung phone and found evidence that it belonged to SY, including:

a. Numerous text messages were found on the Samsung cellphone in which the user of the cellphone sent a text message referencing himself as "millz," which is believed to be SY's nickname in light of his Yahoo email account discussed above.

b. In addition, a text message was found on the cellphone from TELEPHONE NUMBER 2,⁴ which was listed in the Samsung cellphone under J.C.'s first name.⁵ (It subsequently was determined through open sources that TELEPHONE NUMBER 2 is associated with J.B. LLC, a business located in Beltsville, Maryland,⁶ and found within the residence was a

⁴ The actual phone number is known to law enforcement, but is withheld here for purposes of confidentiality.

⁵ J.C.'s true name is known to law enforcement, but is withheld here for purposes of confidentiality.

⁶ The actual business name is known to law enforcement, but is withheld here for purposes of confidentiality.

customer copy of a cashier's check where the remitter was J.B. LLC.) This text message read as follows: "WTF Moussa."

c. Also found on the Samsung cellphone were a series of text messages with TELEPHONE NUMBER 3,⁷ which is believed to belong to SY's sister, M.S.,⁸ in which the Samsung cellphone user sent TELEPHONE NUMBER 3 the email address of MILLZ.MUGGA@YAHOO.COM and M.S. replied a few moments later, asking the Samsung cellphone user to check his email. Therefore, I will hereinafter refer to the phone as "SY'S PHONE."

41. Furthermore, while searching SY's PHONE, the following evidence was identified:

a. The Internet history found on SY's PHONE indicated that the user of the cellphone had visited *brainsdumps.ru* numerous time and placed orders for payment card numbers. Based on my training and experience, I know that *brainsdumps.ru* is a Russian-based website that sells fraudulently or illegally obtained payment card numbers.

b. Numerous text messages from various telephone numbers to SY'S PHONE in which four digit numbers were provided. Based on my training and experience, it appears that these numbers are the last four digits of payment card numbers embedded onto gift cards. This belief is supported by the fact that many of the gift cards recovered from the Arlington County hotel room on or about May 21, 2015, had four digit numbers written on them, some of which had been crossed out. Law enforcement's investigation indicates that many of the four digit

⁷ The actual phone number is known to law enforcement, but is withheld here for purposes of confidentiality.

⁸ M.S.'s true name is known to law enforcement, but is withheld here for purposes of confidentiality.

numbers that were not crossed out corresponded to the last four digits of the payment card numbers found embedded onto the gift cards' magnetic stripes. It is reasonable to conclude that the markings on the gift cards was a method for tracking the payment card numbers embedded onto the gift cards so as to prevent embedding a payment card number onto a gift card stripe that already had an embedded payment card number on it.

c. Text messages that indicate SY was kept apprised of the money being made off of the gift cards embedded with payment card numbers. For example, on or about March 10, 2016, TELEPHONE NUMBER 4 sent the following text messages to SY's PHONE:⁹

TELEPHONE NUMBER 4:	8956
TELEPHONE NUMBER 4:	800
TELEPHONE NUMBER 4:	0246
TELEPHONE NUMBER 4:	8361
TELEPHONE NUMBER 4:	7406
TELEPHONE NUMBER 4:	1200yaboy--1600me-- 400manny
TELEPHONE NUMBER 4:	0248 600
TELEPHONE NUMBER 4:	7406---9064 400manny
TELEPHONE NUMBER 4:	400--200
TELEPHONE NUMBER 4:	4800
TELEPHONE NUMBER 4:	1600 ...you boy...myboy 1000—gazamon

⁹ The actual phone number is known to law enforcement, but is withheld here for purposes of confidentiality.

TELEPHONE NUMBER 4: 5000 everything dead we on
way bak

TELEPHONE NUMBER 4: 1100 yesterday i got 3500

Likewise, on or about March 18, 2016, TELEPHONE NUMBER 5 sent a text message to the SY'S PHONE that stated: "What I'm giving mark 40 percent he only did a stack the other guy did 1200." This was followed by the text message asking, "what percent should I give him 20 or 30."¹⁰

d. Text messages indicating that SY'S PHONE had assembled teams of individuals for making purchases with the gift cards encoded with third parties' payment card information. For instance, between on or about March 12, 2016, and April 26, 2016, the user of SY'S PHONE communicated with TELEPHONE NUMBER 6 as follows:¹¹

SY'S PHONE: Millz

TELEPHONE NUMBER 6: I'm in Pennsylvania with
team bro

TELEPHONE NUMBER 6: Station

SY'S PHONE: Ard let me know u need pcs

TELEPHONE NUMBER 6: 6 car 13 people my team is in

TELEPHONE NUMBER 6: We r ready bro

TELEPHONE NUMBER 6: I promise

TELEPHONE NUMBER 6: This is a million dollars team

¹⁰ The actual phone number is known to law enforcement, but is withheld here for purposes of confidentiality.

¹¹ The actual phone number is known to law enforcement, but is withheld here for purposes of confidentiality.

TELEPHONE NUMBER 6: Bro I know you very busy but
bro at least

TELEPHONE NUMBER 6: I have 13 people 6 car and all
of them

TELEPHONE NUMBER 6: 514891

TELEPHONE NUMBER 6: 422695

TELEPHONE NUMBER 6: 414720

TELEPHONE NUMBER 6: Frri bro I really need u
tomorrow

TELEPHONE NUMBER 6: Ready

TELEPHONE NUMBER 6: So do I really have to wait on
tj

SY's PHONE: U still there

TELEPHONE NUMBER 6: Yes sir working hard bro

SY's PHONE: Call when the day over !!!

TELEPHONE NUMBER 6: God Bless

TELEPHONE NUMBER 6: Still thankful for the
knowledge I have

SY's PHONE: Yo

TELEPHONE NUMBER 6: Can please bro send dat bin
again¹²

¹² Based upon my training and experience, the term "BIN" is short for "Bank Identification Number." A BIN is the first six digits of a payment card number that identify the payment card by type (e.g., Visa, MasterCard, American Express, etc.) and the issuing bank (e.g., Bank of America, Wells Fargo, Chase, etc.). Suspects involved in payment card fraud often times purchase payment card numbers by their BIN from various payment card websites because some people believe BINs are more susceptible to fraud and/or are more profitable.

SY's PHONE:

402451 good luck

Evidence SY was the Occupant of the Residence

42. Evidence uncovered from the search warrant appears to show that SY also was residing at the residence, including:

a. During the execution of the search warrant, SY was found within the Beltsville residence. Law enforcement recovered various identifying documents, including a Washington, D.C. re-entry identification card in the name of "Moussa Niaky Sy."

b. M.S. arrived at the Beltsville residence during law enforcement's execution of the search warrant. She was in possession of a key to the residence and stated she was there to check on her brother, *i.e.*, SY.

c. Also found within the residence was various paperwork, such as letters and a U.S. Postal Service customs declaration form, associated with J.C. Text messages were found on SY'S PHONE in which the phone's user and TELEPHONE NUMBER 2 discuss rent payments for the Beltsville residence.

d. Furthermore, on or about May 10, 2016, the user of SY'S PHONE sent a text message to a phone number indicating that his address was the Beltsville, Maryland residence.

III. The APPLE IPHONE WITH SERIAL NUMBER C8QPPQBZG5MP

43. On or about April 23, 2017, law enforcement discovered that KAMARA had "posted," a photograph onto his Instagram Account of _mrwallst. This photograph was of a ticket for a Chris Brown concert at the Verizon Center on April 23, 2017, at 1930 hours. The photograph showed that the ticket was for row P Seat 20.

44. The investigating law enforcement contacted the Metropolitan Police Department and requested that they and Verizon Security Team attempt to location KAMARA.

45. KAMARA was taken into custody and then custody of KAMARA along with his belongings was transferred to Special Agent Hitchcock of the FBI and Detective Bamford of Arlington Police Department.

46. When the FBI and the Arlington County Police took custody of KAMARA, it also took custody of the items Metropolitan police had seized, including the TARGET IPHONE and placed them in storage at the Arlington County Police Department Property Section at 1425 North Courthouse Road in Arlington, Virginia 22201.

47. The iPhone remains in storage at the Arlington County Police Department Property Section at 1425 North Courthouse Road in Arlington, Virginia 22201. In my training and experience, I know that the iPhone has been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the iPhone first came into the possession of the FBI and the Arlington County Police Department.

IV. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

48. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

49. ***Electronic Storage.*** There is probable cause to believe that things that were once stored on the iPhone and HP Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that files or remnants of files can be recovered months or even years after they have been downloaded onto an electronic device, deleted, or viewed via the Internet. Electronic files downloaded to an electronic device can be stored for years at little or no cost. Even when files have been deleted,

they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the electronic device until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the electronic device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, an electronic device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, electronic devices—in particular, devices with internal hard drives—contain electronic evidence of how an electronic device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

50. ***Forensic Evidence.*** As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the iPhone and HP Flash Device were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the iPhone and HP Flash Device because:

a. Data on electronic devices can provide evidence of a file that was once on the electronic device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on electronic devices that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the electronic device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Electronic file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on an electronic device that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the media and the application of knowledge about how an electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic device.

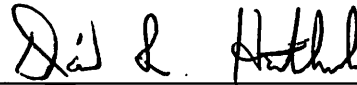
51. ***Nature of Examination.*** Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

52. ***Manner of Execution.*** Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

V. CONCLUSION

53. Based on the foregoing, as well as the training and experience of other law enforcement personnel with whom I have spoken and my own experience, it is my belief that the iPhone contains communications and documents related to records that constitute evidence of the aforementioned crimes, and those items listed in Attachment B, which is incorporated herein by reference. Accordingly, I request that the Court issue the proposed search warrant.

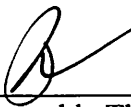
Respectfully submitted,



Special Agent David L. Hitchcock
Federal Bureau of Investigation

Reviewed by Kellen S. Dwyer

Subscribed and sworn to before me
on this 28 day of April, 2017/s/



Theresa Carroll Buchanan
United States Magistrate Judge

Honorable Theresa C. Buchannan
United States Magistrate Judge

ATTACHMENT A

The electronic devices to be searched are an Apple iPhone with serial number C8QPPQBZG5MP, hereinafter the "TARGET IPHONE." The TARGET IPHONE currently is located at the Arlington County Police Department's Property Section at 1425 North Courthouse Road in Arlington, Virginia 22201.

This warrant authorizes the forensic examination of the TARGET IPHONE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the TARGET IPHONE described in Attachment A that relate to violations of Title 18, U.S. Code, §§ 1343 (wire fraud) and 1349 (conspiracy to commit wire fraud), and involve KAMARA and KAMARA co-conspirators, including:

a. All documents, communications or other information related to the gathering, purchase, theft, sale or use of identities and personal identifying information, including records of Internet activity, such as Internet Protocol (“IP”) addresses, browser history, caches, cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

b. All documents, communications or other information related to the transferring or attempted transferring, of money by wire, between bank accounts and/or by or between credit card processing accounts, including the nature, source, destination, and use of those funds.

c. All documents, communications or other information related to the purchase, creation, transmission, or use of stolen, falsified, or fake credit cards, debit cards or other access devices.

d. All documents, communications or other information related to the obtaining, using, selling, or transmitting of stolen, fake or falsified personal identifying information or financial information, including but not limited to names, Social Security numbers, dates of birth, addresses, credit card numbers, and bank accounts.

e. All documents, communications or other information related to the structuring or other concealment of transfers and/or withdrawals.

f. All documents, communications or other information regarding the usernames, phone numbers, emails, Skype or instant messenger names used by the co-conspirators and/or

their associates to transmit information, including personally identifiable information (“PII”), credit card numbers, and false identification documents used in the scheme.

g. All communications with co-conspirators and accomplices and all photographs showing members of the conspiracy.

2. Evidence of user attribution showing who used or owned the TARGET IPHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as flash memory or other media that can store data) and any photographic form.